REMARKS

The Office Action dated March 5, 2008, has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 9, 10, 17, and 23-36 have been amended to more particularly point out and distinctly claim the subject matter of the invention. Claims 11-13 have been canceled without prejudice or disclaimer. Claims 37-39 are newly added. No new issues have been raised. Claims 1-10 and 14-39 are presently pending.

The Office Action indicated that claims 21, 22, 27, 28, 34 and 35 have been allowed. Applicants wish to thank the Examiner for allowing these claims. However, claims 1-20, 23-26, 29-33 and 36-44 are respectfully submitted for reconsideration.

Claims 1-2, 7-10, 13, 14, 20, 23, 24, 29-31 and 36 were rejected under 35 U.S.C. §102(e) as being anticipated by Irwin (U.S. Patent Publication No. 2002/0204728). The Office Action took the position that Irwin discloses all of the elements of the claims. This rejection is respectfully traversed for at least the following reasons.

Claim 1, from which claims 2-9 depend, is directed to a method. Routing information is extracted from a received message at a border between a first network and a second network. At least one invalid entry is added to first-network entries of the routing information to blurr or hide an actual number of routing entries which correspond to routing nodes through which the received message has been routed. The first-network entries relate to a routing path of the message within the first network. An encrypted routing information is generated by encrypting the at least one invalid entry and the first-

network entries by using an own token at least for each of the first-network entries. Routing information of the received message is replaced by the encrypted routing information. The received message is forwarded with the encrypted routing information to the second network.

Claim 10 is directed to an apparatus. An extracting means is configured for extracting the routing information from a received message at a border between a first network and a second network. An adding means is configured for adding at least one invalid entry to first-network entries of the routing information in order to blurr or hide an actual number of routing entries which correspond to routing nodes through which the received message has been routed. The first-network entries relate to a routing path of the message within the first network. An encrypting means is configured for generating an encrypted routing information by encrypting the at least one invalid entry and the first-network entries by using an own token at least for each of the first-network entries. A replacing means is configured for replacing the routing information of the received message by the encrypted routing information. A forwarding means is configured for forwarding the received message with the encrypted routing information to the second network.

Claim 14, from which claims 15-23 depend, is directed to a method. Routing information is extracted from a received message at a border between a first network and a second network. A decrypted and reversed routing information is generated by decrypting a tokenized second-network entry relating to a routing path of the message within the second network. The content of the decrypted second-network entry is also

reversed. The routing information of the received message is replaced by the decrypted and reversed routing information. The received message is forwarded with the decrypted and reversed routing information to the second network.

Claim 24, from which claims 25-29 depend, is directed to an apparatus. An extracting means is configured for extracting routing information from a received message at a border between a first network and a second network. A decrypting and reversing means is configured for generating decrypted and reversed routing information, by decrypting a tokenized second-network entry relating to a routing path of the message within the second network, and reversing the content of the decrypted second-network entry. A replacing means is configured for replacing the routing information of the received message by the decrypted and reversed routing information. A forwarding means is configured for forwarding the received message with the decrypted and reversed routing information to the second network.

Claim 30, from which claims 37-39 depend, is directed to an apparatus. An extractor is configured to extract routing information from a received message at a border between a first network and a second network. An adder, operably connected to the extractor, is configured to add at least one invalid entry to first-network entries of the routing information to blurr or hide an actual number of routing entries which correspond to routing nodes through which the received message has been routed. The first-network entries relate to a routing path of the message within the first network. An encryptor, operably connected to the extractor, is configured to generate encrypted routing information by encrypting the at least one invalid entry and the first-network entries, by

using an own token at least for each of the first-network entries. A replacer, operably connected to the extractor, is configured to replace the routing information of the received message by the encrypted routing information. A transmitter, operably connected to the extractor, is configured to forward the received message with the encrypted routing information to the second network.

Claim 31, from which claims 32-36 depend, is directed to an apparatus. An extractor is configured to extract the routing information from a received message at a border between a first network and a second network. A decryptor, operably connected to the extractor, is configured to generate a decrypted and reversed routing information by decrypting a tokenized second-network entry relating to a routing path of the message within the second network and further configured to reverse the content of the decrypted second-network entry. A replacer, operably connected to the extractor, is configured to replace the routing information of the received message by the decrypted and reversed routing information. A transmitter, operably connected to said extractor, is configured to forward the received message with the decrypted and reversed routing information to the second network.

As will be discussed below, the teachings of Irwin fail to disclose or suggest all of the elements of the claims, and therefore fails to provide the features discussed above. The rejection is respectfully traversed for at least the following reasons.

Irwin discloses a method of cryptography that generates a special value that relates to a communications packet. The special value is hidden in a field of a packet header of a communications packet. Referring to FIG. 1, a source node 12 is connected to an

intermediary node 14 via a communications link 16. The source node 12 computes a cryptographic special value 30 for each packet to be transmitted by using a shared secret key (SSK) that is know by the source node 12 and intermediary node 14. The special value 30 is hidden in one or more fields 26 within the header portion 22 of each packet to be transmitted (see paragraph [0022] of Irwin).

The packet 20 is then transmitted over the network 18 towards the destination node 14. The destination node 14 will compute a cryptographic special value 30' using the shared secret key and will compare the special value 30' to the original special value received 30. If the special values (30 and 30') match, the destination intermediary node 14 has successfully authenticated the transmitted packet 20.

The Office Action wrongfully concluded that paragraph [0010] of Irwin discloses the claimed feature of "adding at least one invalid entry to first-network entries of said routing information to blur or hide an actual number of routing entries which correspond to routing nodes through which said received message has been routed, said first-network entries relating to a routing path of said message within said first network", as recited in independent claim 1, and similarly in independent claims 10, 14, 24, 30 and 31. Referring to claim 1, routing information is extracted from a received message at a border between first and second networks. Claim 1 also recites adding at least one invalid entry to first network entries of the routing information that was extracted. Furthermore, claim 1 recites that the at least one invalid entry is added to <u>blur or hide an actual number of routing entries</u> which correspond to routing nodes through which the received message has been routed (emphasis added).

The Office Action relied on the Abstract and paragraph [0010] of Irwin as allegedly disclosing the above identified subject matter of claim 1. Applicants disagree and submit that the Abstract is limited to an authentication scheme that includes a sending node and receiving node authenticating a packet by using cryptography to avoid network intrusion by third parties. As for the teachings of paragraph [0010] of Irwin, the subject matter discussed in paragraph [0010] is nearly identical to the teachings of the Abstract.

The method of hiding information from outside third party intrusion, as disclosed in Irwin, is limited to the prevention of third parties from recovering the information contained in the packets. The mere hiding of information from third parties who are unable to decipher packet encryption, as disclosed in Irwin, cannot be regarded as teaching the subject matter recites in the claims. For example, claim 1 recites extracting routing information and adding at least one invalid entry to blur or hide an actual number of routing entries which correspond to routing nodes through which the received message has been routed. The disclosure of Irwin is not concerned with blurring or hiding an actual number of routing entries of a packet. Furthermore, the hiding operation performed by Irwin is only used to hide the information in the packet from third party intrusion, the hiding operation does not change any information in the packet. No information is added or changed by the cryptography performed by Irwin.

Irwin does not teach or recite "adding at least one invalid entry to first-network entries of said routing information to blur or hide an actual number of routing entries which correspond to routing nodes through which said received message has been routed,

said first-network entries relating to a routing path of said message within said first network", as recited in independent claim 1, and similarly in independent claims 10, 14, 24, 30 and 31.

Therefore, Applicants submit that Irwin fails to teach all of the subject matter of independent claims 1, 10, 14, 24, 30 and 31. By virtue of dependency, Irwin also fails to teach the subject matter of dependent claims 2-9, 15-23, 25-29, and 32-39. Withdrawal of the rejection of claims 1, 2, 7-10, 13, 14, 20, 23, 24, 29-31 and 36 is kindly requested.

Claims 3, 11, 16 and 25 were rejected under 35 U.S.C. §103(a) as being unpatentable over Irwin in view of Yla-Outinen et al. (U.S. Patent Publication No. 2004/0152469). This rejection is respectfully traversed. Claim 11 has been cancelled thus rendering its rejection moot.

Irwin is discussed above. Yla-Outinen discloses a method and a system for controlling a processing load in a packet data network, wherein a load control information is set in a predetermined field of a message. The load control information is then checked on the routing path of the message and a processing resource of the packet data network is selected in response to the result of a checking step. Load balancing information can be provided at the network to provide a balancing and load sharing function without heavy string comparisons and data base queries.

Claims 3, 16 and 25 are dependent upon claims 1, 14 and 24 and contain all of the limitations thereof. As discussed above, Irwin fails to disclose or suggest all of the elements of claims 1, 14 and 24. In addition, Yla-Outinen fails to cure the deficiencies in Irwin as Jensen also fails to disclose or suggest "adding at least one invalid entry to first-

network entries of said routing information to blurr or hide an actual number of routing entries which correspond to routing nodes through which said received message has been routed, said first-network entries relating to a routing path of said message within said first network", as recited in independent claim 1, and similarly in independent claims 10, 14, 24, 30 and 31. Thus, the combination of Irwin and Yla-Outinen fails to disclose or suggest all of the elements of claims. Furthermore, claims 3, 16 and 25 should be allowed for at least their dependence upon claims 1, 14 and 24 and for the specific limitations recited therein.

Claims 4-6 and 17-19 were rejected under 35 U.S.C. §103(a) as being unpatentable over Irwin in view of Jensen et al. (U.S. Patent No. 6,185,612). This rejection is respectfully traversed.

Irwin is discussed above. Jensen discloses a method for managing and using topology information in a network. A topology information manager keeps fragments of network topology and provides access to entire fragments or to fragment summaries in response to authenticated requests. An authenticated path selector uses topology information from the manager to select message routes. The path selector may use summaries of hidden network paths to determine whether the hidden path is desirable, without having access to all topological information about the hidden path. Messages may be forwarded over hidden paths by the manager without disclosing more than the summary information to the message provider.

Claims 4-6 and 17-19 are dependent upon claims 1 and 14 and contain all of the limitations thereof. As discussed above, Irwin fails to disclose or suggest all of the

elements of claims 1 and 14. In addition, Jensen fails to cure the deficiencies in Irwin as Jensen also fails to disclose or suggest "adding at least one invalid entry to first-network entries of said routing information to blurr or hide an actual number of routing entries which correspond to routing nodes through which said received message has been routed, said first-network entries relating to a routing path of said message within said first network", as recited in independent claim 1, and similarly in independent claims 10, 14, 24, 30 and 31. Thus, the combination of Irwin and Jensen fails to disclose or suggest all of the elements of claims. Furthermore, claims 4-6 and 17-19 should be allowed for at least their dependence upon claims 1 and 14 and for the specific limitations recited therein.

For at least the reasons discussed above, Applicants respectfully submit that the cited references fail to disclose or suggest all of the elements of the claimed invention. These distinctions are more than sufficient to render the claimed invention unanticipated and unobvious. It is therefore respectfully requested that all of claims 1-10 and 14-36 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicants' undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Kamran Emdadi
Registration No. 58,823

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

KE/cqc

Enclosures: Petition for Extension of Time
Check No. 19357